

Robocall Mitigation Program Description

GIP Technology Inc.

In accordance with 47 CFR § 64.6305(d), **GIP Technology Inc.** (hereinafter “GIP Technology”) submits this Robocall Mitigation Program description to certify its ongoing compliance with the Pallone-Thune TRACED Act and the Commission’s rules regarding the mitigation of illegal robocalls.

Section 1: General Certification

GIP Technology hereby certifies to the Commission that:

1. **Scope of Program:** GIP Technology has implemented a robocall mitigation program consistent with 47 CFR § 64.6305(a) that applies to all calls it originates on its network.
2. **Status of Prior Filings:** Any prior certification submitted by GIP Technology has not been removed by Commission action, and GIP Technology has not been prohibited from filing in the Robocall Mitigation Database by the Commission.
3. **Disclosure of Prior Wrongdoing:** Pursuant to § 64.6305(d)(2)(iv), GIP Technology certifies that neither itself nor any entity for which it shares common ownership, management, directors, or control has, within the prior two years, been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing related to the transmission of illegal robocalls, spoofing, or deficient certification filings.

Section 2: STIR/SHAKEN Implementation Status

Pursuant to § 64.6305(d)(1), GIP Technology certifies to the following STIR/SHAKEN implementation status:

- **Option A:** It has fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it originates are compliant with § 64.6301.
- **Option B:** It has implemented the STIR/SHAKEN authentication framework on a portion of its network and all calls it originates on that portion of its network are compliant with § 64.6301(a) and (b).
- **Option C:** It has not implemented the STIR/SHAKEN authentication framework on any portion of its network.

Section 3: Reasonable Steps to Avoid Illegal Traffic

Pursuant to § 64.6305(d)(2)(ii), GIP Technology details the specific reasonable steps it has taken to avoid originating illegal robocall traffic:

A. Know Your Customer (KYC) and Upstream Provider Vetting

- **Customer Identity Verification:** GIP Technology verifies the identity of all residential, retail, and wholesale subscribers using standard business practices, including the collection of physical service addresses and business credentials.
- **High-Risk Customer Scrutiny:** GIP Technology applies enhanced due diligence to outbound call centers and high-volume origination services, including a stricter application review process and ongoing traffic monitoring.
- **Upstream Provider Verification:** GIP Technology maintains comprehensive knowledge of all carriers from which it receives traffic. GIP Technology verifies that all upstream providers with which it exchanges traffic are registered and appear in good standing in the FCC's Robocall Mitigation Database. Basic identification details (business location, contact persons, state of incorporation) are collected for all upstream partners.
- **Contractual Obligations:** All new and existing interconnection agreements include provisions explicitly prohibiting the exchange of illegal traffic and mandating cooperation with traceback requests.

B. Caller ID Authentication and Validation

- **Assignment Validation:** Subscribers are permitted to use only telephone numbers directly managed by GIP Technology or obtained through an authorized partner.
 - For single-line subscribers, network elements (e.g., Class 5 switches) are configured to reject calls presenting a Caller ID that does not match the number assigned to that specific subscriber.
 - For Multi-Line Telephone System (MLTS) subscribers, GIP Technology screens originating calls to ensure the originating number matches a number allocated to that customer.

C. Analytics and Blocking Systems

- **Traffic Monitoring:** GIP Technology utilizes network monitoring tools to analyze traffic patterns and identify anomalous behavior indicative of robocall campaigns (e.g., high call volume from a single source, high call-attempt rates to invalid numbers).

- **Third-Party Analytics:** GIP Technology utilizes third-party analytics vendors to assist in identifying and blocking illegal traffic.
- **Investigation and Remediation:** Upon identification of suspicious patterns, GIP Technology initiates an investigation. If illegal robocall activity is confirmed, GIP Technology takes appropriate remedial action, which may include warnings, traffic filtering, or termination of service.

Section 4: Traceback Response Commitment

Pursuant to § 64.6305(d)(2)(iii), GIP Technology makes the following formal commitments regarding traceback:

- **Designated Point of Contact:** GIP Technology has designated a single point of contact responsible for addressing robocall mitigation and traceback issues, as filed in the Robocall Mitigation Database portal per § 64.6305(d)(4)(v).
 - **24-Hour Response:** GIP Technology commits to responding fully to all traceback requests originating from the Commission, law enforcement, and the industry traceback consortium (e.g., USTelecom) within **twenty-four (24) hours** of receipt.
 - **Full Cooperation:** GIP Technology commits to cooperating fully with such entities to investigate the source of illegal traffic and to take immediate steps to stop any illegal robocallers that use its service to originate calls.
-